Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 29 April 2019 – Friday 17 May 2019

Supervised hours: 5 hours | Paper Reference **20158K**

Information Technology

Unit 11: Cyber Security and Incident Management

Part A

You must have:
Risk_Assessment.rtf
Security_Plan.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this paper is 43.

Turn over ▶

©2019 Pearson Education Ltd.

Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of three weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour, **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name] _U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J _U11A

Each learner will need to submit 3 PDF documents, within their folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 21 May 2019.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name] _U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J _U11A

You will need to submit 3 PDF documents, within your folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand in your work to your teacher/tutor.

BLANK PAGE

Set Task Brief

Projet Serendipity

Projet Serendipity (PS) is an organisation that tries to make links between PhD students. It started when Professor Fred Gorse, an expert in artificial intelligence, met Professeur Adele Lefebvre, who studies complex data processing. Each had developed some computing techniques that the other might find useful in their own work.

Adele thought it might make an interesting PhD project to try and link up areas of research where the people involved would not normally meet. Adele and Fred then started a joint project between their universities.

The first students produced some interesting results and the project expanded as more university departments heard about it. The project eventually involved PhD students from over 20 universities around the world.

In 2018, Fred and Adele decided that the administration of the project was too complicated. They decided that PS should become an independent, non-profit organisation. PS would still get PhD students from universities and would be funded by grants and subscriptions.

The Pan-Europe Foundation for Education Research (PEFER), based in Lille, France, agreed to house PS in a row of four rooms on the second floor of its premises, **Figure 1**. PS will have meeting rooms and workspace but most PhD students will work from home, accessing the servers and data stores remotely.

Fred and Adele are joint Chief Executives of the new PS board of directors. Other members were elected from the present students and their supervisors. Fred and Adele provide oversight and continuity, other board members deal with the day-to-day running of PS and its research programme. A PhD typically takes three to four years to complete, so a high turnover of board members is expected. The board will only meet a few times a year.

PS does not have much money, so most of the hardware that will be used to form the PS network in Lille is second-hand, **Figure 2**. This hardware is high quality but quite old. PS has been given:

- A Cisco 7200 router, enterprise level, but out of support from Cisco.
- A NETGEAR ProSAFE WAC730. A wireless access point (WAP) for small and medium-sized enterprises. It uses 802.11ac and will easily cover the PS area providing 100mbp/s. Five years old, it had a lifetime guarantee but this did not transfer to PS.
- Three PCs running Linux. Dating from 2015, these were good quality business PCs when new.
- Three HP BL660c Gen 8 blade servers with mountings, dating from 2014. Each server has 48 cores and is described as ideal for virtualisation, database, and business processing. They have the latest LINUX Enterprise OS. All drivers are up to date.
- A Seagate 4-Bay Network Attached Storage (NAS) unit with four, 5TB removable drives. It is being used by the existing project and contains copies of all the files and data stores. It is currently in Fred's department at his university.

- A networked laser printer and a networked scanner. These are suitable for small office use and only a year old.

Fred and Adele are experts in their own subjects but are inexperienced with cyber security. They decided that someone not in PS should advise them. You have been hired for the task.

At a meeting with Fred and Adele, PEFER's security is explained. The main entrance has a security barrier and is the only unlocked entrance. Guards are on duty from 0700 – 1900 on weekdays, at other times the building is locked. PEFER's business hours are 0900 – 1700 Monday to Friday.

Security staff open the building at 0700, tour the building, put on lights and unlock rooms. The rooms have simple mortice locks. Rooms are usually left unlocked during the day. Service staff lock the rooms each evening when they finish cleaning. Ground floor doors and windows are alarmed when PEFER is closed.

The building is in a low-crime area and PEFER's directors do not want to change current security measures.

Figure 1 shows PS's part of the building.

Figure 2 shows the proposed layout of the PS network.

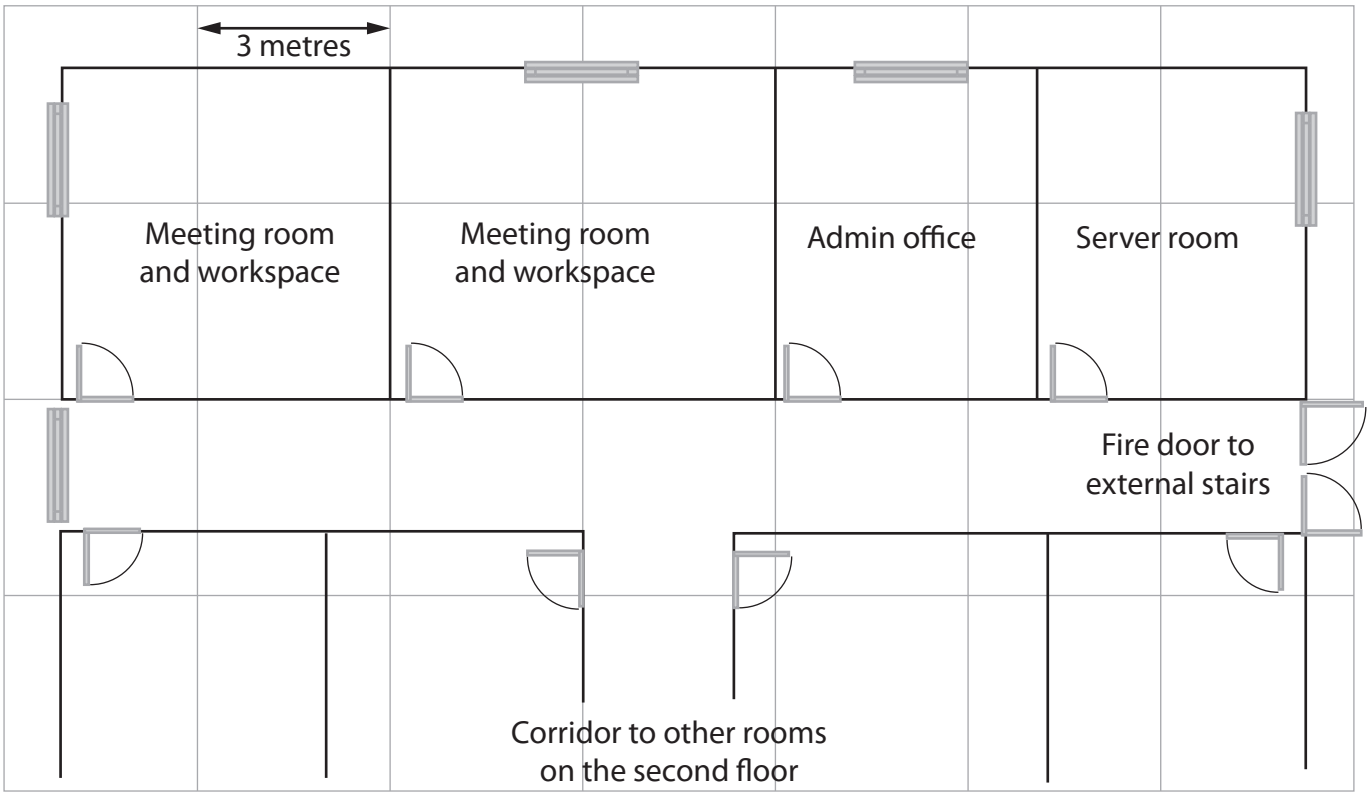

Figure 1

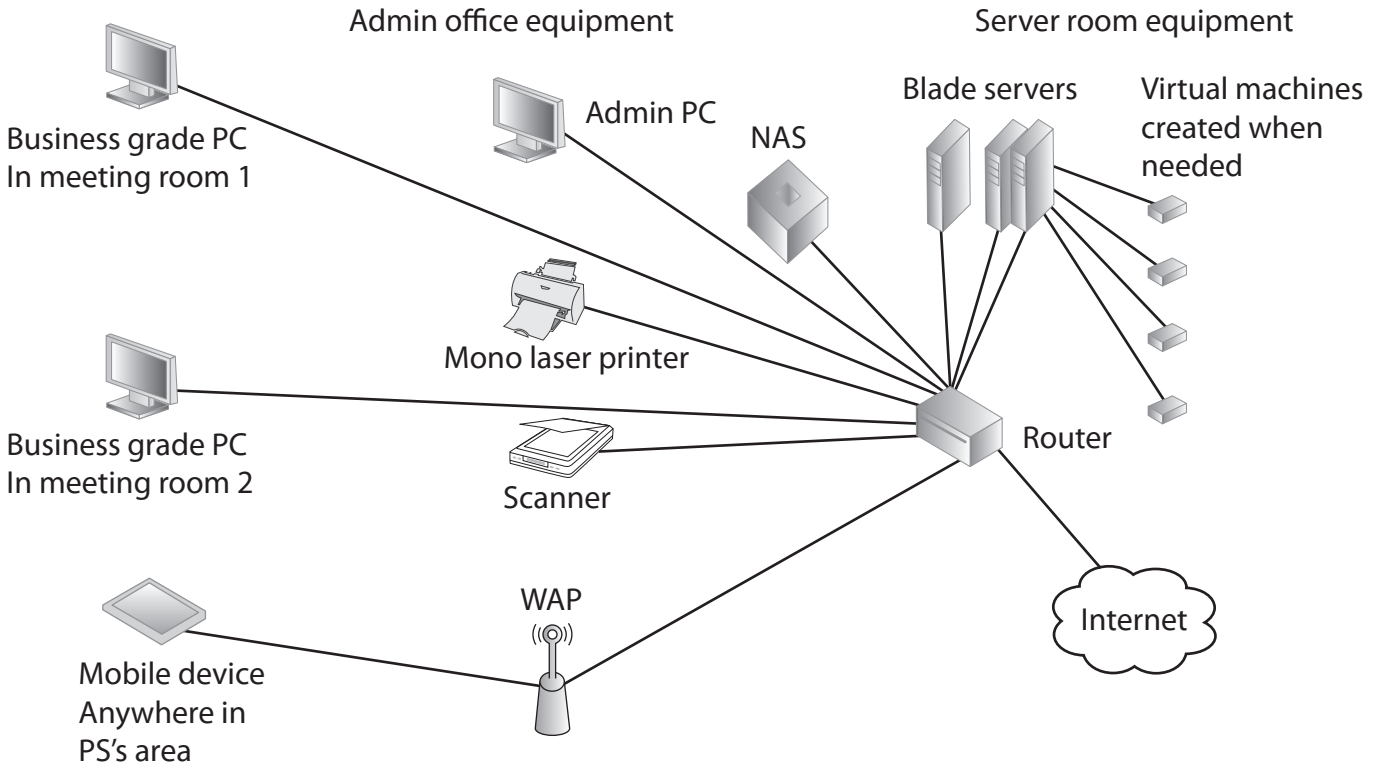

Figure 2

Development plan

During the meeting with Fred and Adele you establish that:

1. The network will follow the network diagram.
2. PEFER will manage the building's security but Adele is concerned about physical security within PS's area.
3. Fred is concerned about clashes between PS's WiFi and PEFER's WiFi.
4. One of the three blade servers will be used for the roles of admin, web and mail server. The other two will be used to host virtual machines for students' projects.
5. The three PCs must be able to connect to the virtual machines. Only the PC in the admin office should be able to connect to the admin server.
6. Anyone requiring a laptop, tablet or other mobile device must bring their own and connect via WiFi.
7. The WiFi must connect mobile devices to the virtual machines but not the admin server.
8. The NAS is configured as RAID 1. A weekly backup is currently made to storage in Adele's university.
9. PS's students and staff are located around the world, so remote access must be available 24/7.
10. PEFER's IT staff will be available during PEFER's office hours. Remote support methods will be used at other times.
11. All documentation will be available in English and French.

Part A Set Task

You must complete ALL activities in the set task.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given computer network.

Activity 1: Risk assessment of the networked system

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

(Total for Activity 1 = 8 marks)

Activity 2: Cyber security plan for the networked system

Using the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure
(b) action(s) to be taken
(c) reasons for the action(s)
(d) overview of constraints – technical and financial
(e) overview of legal responsibilities
(f) overview of usability of the system
(g) outline cost-benefit
(h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan _[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

(Total for Activity 2 = 20 marks)

Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

(Total for Activity 3 = 12 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS
TOTAL FOR PART A = 43 MARKS